UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE
NASHVILLE

UNITY MEDICAL CENTER MANCHESTER a/k/a Coffee Medical Group, LLC and RUSSELLVILLE HOSPITAL, INC., individually, and on behalf of all others similarly situated, Plaintiffs, vs. UNITEDHEALTH GROUP INCORPORATED, OPTUM, INC., and CHANGE HEALTHCARE INC., Defendants.	Civil No._____ **CLASS ACTION COMPLAINT** Jury Trial Demanded

Plaintiffs Unity Medical Center Manchester a/k/a Coffee Medical Group, LLC ("Unity Hospital") and Russellville Hospital, Inc. ("Russellville Hospital") (collectively the "Hospitals") bring this Class Action Complaint against Defendants UnitedHealth Group Incorporated ("United"), Optum, Inc. ("Optum"), and Change Healthcare Inc. ("Change") (collectively, "Defendants") based upon its personal knowledge, investigation by counsel, and review of public documents and states as follows:

INTRODUCTION

1. The Hospitals bring this action for Defendants' failure to timely and adequately process and pay the amounts due for their medical services.

2. Change is a healthcare company that provides payment and revenue cycle services, clinical and imaging services, and other services to its clients. It is a lynchpin of a

system which facilitates the payment of approximately $100 million per day to health care providers, such as hospitals, many of which have limited liquidity.

3. According to the Wall Street Journal, "Change processes around 15 billion transactions a year."[1]

4. The Hospitals seek to hold Defendants responsible for the harms caused and will continue to cause the Hospitals and other similarly situated persons and/ or entities in the massive and preventable cyberattack purportedly discovered by Defendants on February 21, 2024, in which cybercriminals, known as the BlackCat/ALPHV ransomware group, infiltrated Defendants' inadequately protected network and accessed highly sensitive information which was being kept unprotected ("Data Breach").

5. According to the Wall Street Journal, "The hackers who attacked UnitedHealth Group's Change Healthcare unit were in the company's networks for more than a week before they launched a ransomware strike." *See* https://www.wsj.com/articles/change-healthcare-hackers-broke-in-nine-days-before-ransomware-attack-7119fdc6 ("Between Feb. 12 and when the ransomware was detonated on Feb. 21, the hackers were moving laterally within Change's network").

6. Indeed, the Hospitals and Class Members were wholly unaware of the Data Breach until they were unable to access important and sensitive information.

7. As a result of the breach, Change "disconnected [its] systems to prevent further impact," according to its statement released on February 26, 2024. With those systems disconnected, the Hospitals and Class Members have been cut off from over 100 services

[1] https://www.wsj.com/articles/change-healthcare-hackers-broke-in-nine-days-before-ransomware-attack-7119fdc6

provided by Change, including benefits verification, claims submission, and prior authorization. Without those services, the Hospitals and Class Members have not, and cannot, be paid for their work with patients.

8. Defendants disregarded the rights of the Hospitals and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that sensitive information was safeguarded and failing to take available steps to prevent unauthorized disclosure of data and failing to follow applicable, required and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. Defendants further harmed the Hospitals and Class Members by intentionally, willfully, recklessly, and/or negligently implementing procedures to disconnect the services that they rely on to secure payment. the Hospitals and Class Members are entitled to injunctive and other equitable relief.

PARTIES, JURISDICTION, AND VENUE

9. Plaintiff Unity Medical Center Manchester a/k/a Coffee Medical Group, LLC is a corporate citizen of Tennessee. It is a Tennessee non-profit limited liability company that maintains its principal place of business in Manchester, Tennessee. Its only member is Unity Medical Center, Inc., itself a Tennessee corporation that maintains its principal place of business in Manchester, Tennessee.

10. Plaintiff Russellville Hospital, Inc. is a corporate citizen of Tennessee and Alabama. It is a Tennessee non-profit corporation that maintains its principal place of business in Russellville, Alabama.

11. Defendant UnitedHealth Group Incorporated ("United") is a corporate citizen of Minnesota. It is a corporation with a principal place of business located at 9900 Bren Road

East, Hopkins, Minnesota 55343-9664.

12. Defendant Optum, Inc. ("Optum") is a corporate citizen of Minnesota. It is a corporation with a principal place of business located at 11000 Optum Circle, Eden Prairie, Minnesota 55344. Optum is a subsidiary of United.

13. Defendant Change Healthcare Inc. ("Change") is a corporate citizen of Tennessee. It is a corporation with a principal place of business located at 424 Church Street, Suite 1400, Nashville, Tennessee 37219. Change is a subsidiary of Optum.

14. Jurisdiction is proper in this Court under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendants.

15. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

16. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to the Hospitals' claims took place within this District and Defendants conduct business in this Judicial District.

FACTUAL ALLEGATIONS

17. On February 21, 2024, Change failed to prevent a cyberattack affecting a number of its systems and services (the "Data Breach"). At 4:27 PM EST, it announced that it was "experiencing a network interruption related to a cyber security issue," that it had disconnected its systems, and that disruption to its services was expected to last at least through the day.

18. According to the Wall Street Journal, "The hackers who attacked UnitedHealth Group's Change Healthcare unit were in the company's networks for more than a week before

they launched a ransomware strike." *See* https://www.wsj.com/articles/change-healthcare-hackers-broke-in-nine-days-before-ransomware-attack-7119fdc6 ("Between Feb. 12 and when the ransomware was detonated on Feb. 21, the hackers were moving laterally within Change's network … The length of time the attackers were in the network suggests they might have been able to steal significant amounts of data from Change's systems.")

19. As a result of Change's failures, hospitals and other medical providers, including the Hospitals and Class Members, have been unable to receive payment for their services. As many Class Members, including the Hospitals, have limited liquidity, this disruption threatens to bankrupt hundreds if not thousands of care providers, if it hasn't done so already.

20. Change is a health software services company which provides payment and revenue cycle services, clinical imaging services, and other services to its clients. It is a large player in the healthcare sector, as its services allow health care providers to resolve payments for their care. It handles 15 billion healthcare transactions totaling more than $1.5 trillion annually. According to the Department of Justice, it handles 50 percent of all medical claims in the United States.

21. The Hospitals and Class Members are medical providers who have suffered delays in processing claims and revenue cycle services as a result of the Data Breach.

22. On March 1, 2024, U.S. Senator Charles Schumer sent a letter to the Centers for Medicare & Medicaid Services explaining that a result of the cyberattack: "Hospitals are struggling to process claims, bill patients, and receive electronic payments, leaving them financially vulnerable. Many hospitals are approaching a financial cliff where they will no longer be able to rely on their cash on hand."[2]

[2] https://www.democrats.senate.gov/imo/media/doc/ces_-_cms_response_change_healthcare_outage_3-1-

23. On March 4, 2024, The American Hospital Associations ("AHA") sent a letter to Congress stating:

> Unfortunately, UnitedHealth Group's efforts to date have not been able to meaningfully mitigate the impact to our field. Workarounds to address prior authorization, as well as claims processing and payment are not universally available and, when they are, can be expensive, time consuming and inefficient to implement. For example, manually typing claims into unique payer portals or sending by fax machine requires additional hours and labor costs, and switching revenue cycle vendors requires hospitals and health systems to pay new vendor fees and can take months to implement properly.[3]

24. In addition, the AHA explained to Congress that the funding assistance program United claims is helpful, is not:

> In addition, UnitedHealth Group's "Temporary Funding Assistance Program" that it stood up as part of its response on March 1 will not come close to meeting the needs of our members as they struggle to meet the financial demands of payroll, supplies and bond covenant requirements, among others.

Id.[4]

25. On March 19, 2024, the AHA again sent a letter to Congress explaining that is had conducted a survey of approximately 1,000 hospitals, concerning the cyberattacks impact, and explained:

> Change Healthcare's downed systems are hampering providers' ability to verify patients' health insurance coverage, process claims and receive payment from many payers, exchange clinical records with other providers, provide cost estimates and bill patients, and, in some instances, access the clinical guidelines used in clinical decision support tools and as part of the prior authorization process. The staggering loss of revenue means that some hospitals and health systems may be unable to pay salaries for clinicians and other members of the care team, acquire necessary medicines and supplies, and pay for mission critical contract work in areas such as physical security, dietary and

24pdf.pdf

[3] *See* https://www.aha.org/lettercomment/2024-03-04-aha-urges-congress-provide-support-help-minimize-further-fallout-change-healthcare-attack.

[4] https://www.optum.com/en/business/providers/health-systems/payments-lending-solutions/optum-pay/temporary-funding-assistance.html (explaining Temporary Funding Assistance Program for providers).

> environmental services. In addition, replacing previously electronic processes with manual processes has often proved ineffective and is adding considerable administrative costs on providers, as well as diverting team members from other tasks.

26. According to AHA's March 2024 survey (titled: "AHA Survey: Change Healthcare Cyberattack Significantly Disrupts Patient Care, Hospitals' Finances") of nearly 1,000 hospitals concerning the cyberattack:

> (1)
>
> "74% of hospitals report direct patient care impact. Nearly 40% report patients having difficulty accessing care because of delays in processing of health plan utilization requirements (e.g. prior authorization)."[5]
>
> (2)
>
> "94% of hospitals report financial impact, with more than half reporting 'significant or serious' impact. 82% of hospitals report impacts on their cash flow. Of these: More than 33% report impact to more than half of their revenue. Nearly 60% report that the impacts to revenue is $1 million per day of greater. 44% report they expect the negative impact on revenue to continue for 2-4 more months. There is still substantially uncertainty over revenue cycle impacts, with more than 20% currently uncertain of the magnitude of the impacts."[6]

27. On April 16, 2024, the House Energy and Commerce Committee held a hearing entitled "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack." According to a Committee Press Release, "This hearing will give Members the opportunity to hear from industry experts from across the health care system on what more needs to be done to secure patients' sensitive health information and protect our health care sector from disruption."[7]

---

[5] https://www.aha.org/system/files/media/file/2024/03/aha-survey-change-healthcare-cyberattack-significantly-disrupts-patient-care-hospitals-finances.pdf

[6] *Id*.

[7] https://energycommerce.house.gov/posts/chairs-rodgers-and-guthrie-announce-health-subcommittee-hearing-on-health-care-cybersecurity.

28. On May 1, 2024, the Senate Finance Committee held a hearing concerning the cyberattack. The only witness was Andrew Witty, CEO of UnitedHealth Group. According to Senator Wyden:

> In the wake of the hack, United essentially disconnected Change from the rest of the health care system. It took weeks for Change to get back online, leaving health care providers in a state of financial bedlam. Doctors and hospitals went weeks delivering services but without getting paid. Insurance companies couldn't reimburse providers. Even today, key functions supporting plans and providers, including sending receipts for services that have been paid and the ability to reimburse patients for their out of pocket costs, are not back up and running.
>
> …
>
> Mr. Witty owes Americans an explanation for how a company of UHG's size and importance failed to have multi-factor authentication on a server providing open door access to protected health information, why its recovery plans were so woefully inadequate and how long it will take to finally secure all of its systems.[8]

29. On May 1, 2024, Mr. Witty also testified before the House Energy and Commerce Committee and stated approximately one-third of Americans may have been compromised by the cyberattack and that Change paid a $22 million ransom to hackers.

30. In his opening statement to the Committee, Mr. Witty acknowledged "As a result of this malicious cyberattack, patients and providers have experienced disruptions and people are worried about their private health data. To all those impacted, let me be very clear: I am deeply sorry."

31. Given that it is a company in which half of America's medical payments flow, Change needs to maintain the utmost security of its systems. Indeed, Change states on its website that "[w]e implement and maintain organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction,

[8] https://www.finance.senate.gov/imo/media/doc/0501_wyden_statement.pdf.

loss, alteration, or misuse."[9] As a sophisticated business entity, making promises that its systems were safe and secure, Change knew it needed to adequately protect those systems. It failed to do so.

32. According to reports, Change allowed its data and systems to be encrypted by the "Blackcat" ransomware gang, affiliated with AlphV. Ransomware attacks encrypt a target's computer systems in a manner that prevents the target from gaining access to their material, unless a ransom is paid in return for the passcode required to decrypt the system. It is a common form of cyberattack, and one that Change should have known it would be threatened with.

33. Defendant Change did not use reasonable security procedures and practices suited to the sensitive information they were maintaining. Worse, it compounded the attack by disconnecting all of its services, even though reports indicate that only certain systems were affected. By disconnecting all services, Change guaranteed that no medical providers could be paid for their services.

34. Given the nature of the healthcare sector, many medical providers especially hospitals, like the Hospitals, are forced to rely on prompt payment of claims in order to operate their businesses.

35. Unity Hospital is paid weekly from insurance companies to settle its charges for services. Unity Hospital is unable to secure this payment due to Change's system lockout, and thus has been denied millions of dollars as of May 2024, a figure that will continue to rise day after day.

36. Russellville Hospital is paid weekly from insurance companies to settle its charges for services. Unity Hospital is unable to secure this payment due to Change's system

[9] https://www.changehealthcare.com/privacy-notice.

lockout, and thus has been denied millions of dollars as of May 2024, a figure that will continue to rise day after day.

37. Had Change adequately secured its systems this large amount would have been timely paid, as the Hospitals had every reason to expect.

CLASS ACTION ALLEGATIONS

38. The Hospitals bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure on behalf of the Hospitals and the following "Class:"

> All health care providers within the United States who have suffered delays in processing claims and revenue cycle services as a result of the Data Breach reported by Defendants on February 21, 2024.

39. Alternatively, the Hospitals bring this action on behalf of the following "Class:"

> All hospitals within the United States who have suffered delays in processing claims and revenue cycle services as a result of the Data Breach reported by Defendants on February 21, 2024.

40. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers, and directors and any entity in which Defendants has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsel, and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

41. This action has been brought and may properly be maintained as a class action under Fed. R. Civ. P. 23 because there is a well-defined community of interest in the litigation and membership of the proposed Class is readily ascertainable.

42. **Numerosity**: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Class are so numerous that joinder of all members is impractical, if not impossible. The Hospitals are informed and believe and, on that basis, allege that the total number of Class Members is in the thousands of individuals. Membership in the Class will be determined by analysis of Defendants' records.

43. **Commonality**: The Hospitals and the Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

i. Whether Defendants knew or should have known of the susceptibility of their data security systems to a data breach;

ii. Whether Defendants' security procedures and practices to protect their systems were reasonable in light of the measures recommended by data security experts;

iii. Whether Defendants' failure to implement adequate data security measures allowed the Data Breach to occur;

iv. Whether Defendants failed to comply with their own policies and applicable laws, regulations and industry standards relating to data security;

v. Whether Defendants adequately, promptly and accurately informed the Hospitals and Class Members about the Date Breach;

vi. How and when Defendants actually learned of the Data Breach;

vii. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in losses;

viii. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

ix. Whether Defendants engaged in unfair, unlawful or deceptive practices;

x. Whether the Hospitals and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory

relief and/or an accounting is/are appropriate as a result of Defendants' wrongful conduct;

xi. Whether the Hospitals and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

44. **Typicality**: The Hospitals' claims are typical of the claims of the the Hospitals' Class. The Hospitals and all members of the the Hospitals Class sustained damages arising out of and caused by Defendants' common course of conduct in violation of law, as alleged herein.

45. **Adequacy of Representation**: The Hospitals in this class action is an adequate representative of each of the the Hospitals Class in that the Hospitals have the same interest in the litigation of this case as the Class Members, are committed to the vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. the Hospitals is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Class in their entirety. the Hospitals anticipates no management difficulties in this litigation.

46. **Superiority**: The damages suffered by individual Class Members are significant but may be small relative to each member's enormous expense of individual litigation. This makes or may make it impractical for members of the the Hospitals Class to seek redress individually for the wrongful conduct alleged herein. Even if Class Members could afford such individual litigation, the court system could not. Should separate actions be brought or be required to be brought by each individual member of the the Hospitals Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately. Individualized

litigation increases the delay and expense to all parties and to the court system, presented by the case's complex legal and factual issues. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale and comprehensive supervision by a single court.

47. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, so it is impracticable to bring all Class Members before the Court.

48. This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate concerning the Class in their entireties. Defendants' policies and practices challenged herein apply to and affect Class Members uniformly. the Hospitals' challenge of these policies and procedures hinges on Defendants' conduct concerning the Class in their entirety, not on facts or law applicable only to the Hospitals.

49. Unless a Class-wide injunction is issued, Defendants may continue failing to secure private information and proper payment functions.

50. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Fed. R. Civ. P. 23(b)(2).

CLAIMS FOR RELIEF

COUNT I

Negligence

51. The Hospitals realleges the allegations above as if fully set forth herein.

52. At all times herein relevant, Defendants owed the Hospitals and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard that their claims and revenue cycle services would be processed on time and for the correct amounts. Defendants took on this obligation and used their computer systems and networks to ensure that proper payments of claims were to be made.

53. Among these duties, Defendants were expected to provide claims processing and revenue cycle services to the Hospitals using safe and secure computer systems and networks.

54. Defendants owed a duty of care to not subject the Hospitals and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

55. Defendants knew or should have known of the vulnerabilities of their data security systems and the importance of adequate security. Defendants knew or should have known about numerous well-publicized data breaches.

56. Defendants knew or should have known that their data systems and networks did not adequately safeguard the claims processing and revenue cycle services.

57. Only Defendants were in the position to ensure that their systems and protocols were sufficient to protect the Hospitalsand Class Members information.

58. Defendants breached their duties to the Hospitals and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the claims processing and revenue cycle services.

59. Because Defendants knew that a breach of their systems could damage numerous individuals, including the Hospitals and Class Members, Defendants had a duty to adequately

protect their data systems.

60. the Hospitals' and Class Members' willingness to entrust Defendants with their processing needs was predicated on the understanding that Defendants would take adequate security precautions.

61. Defendants also had independent duties under state and federal laws that required Defendants to reasonably to promptly notify them about the Data Breach.

62. Defendants' willful failure to abide by their duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

63. As a proximate and foreseeable result of Defendants' grossly negligent conduct, the Hospitals and Class Members have suffered damages and are at imminent risk of additional harm and damages.

64. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and failure to be able to process claims corrected or timely.

65. Further, explicitly failing to provide timely and clear notification of the Data Breach to the Hospitals and Class Members, Defendants prevented the Hospitals and Class Members from taking meaningful, proactive steps to secure processing needs which caused damages to the Hospitals.

66. There is a close causal connection between Defendants' failure to implement security measures to protect the Hospitals' and Class Members' processing requirements.

67. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

68. The damages the Hospitals and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendants' grossly

negligent conduct.

69. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair […] practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect private information like the processing of confidential claims. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

70. Defendants violated 15 U.S.C. § 45 by failing to use reasonable measures and by not complying with applicable industry standards, as described in detail herein.

COUNT II

Breach of Confidence

71. The Hospitals realleges the allegations above as if fully set forth herein.

72. During the Hospitals' and Class Members' interactions with Defendants, Defendants were fully aware of the important and confidential nature of the processing materials that the Hospitals and Class Members provided to them.

73. As alleged herein and above, Defendants' relationship with the Hospitals and Class Members was governed by promises and expectations that the Hospitals and Class Members' claims processing and revenue cycle service materials would be kept in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third-parties.

74. The Hospitals and Class Members provided their respective claims processing and revenue cycle services to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the materials to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third-parties.

75. The Hospitals and Class Members also provided their claims processing and revenue cycle service materials to Defendants with the explicit and implicit understanding that Defendants would take precautions to protect those materials from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting their networks and data systems and make ensure that claim payments related to the materials would be promptly paid and satisfied.

76. Due to Defendants' failure to prevent, detect and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices to secure the Hospitals' and Class Members' claim processing, the Hospitals' and Class Members' materials were encumbered by and, not able to be used by the Hospitals in the manner expected.

77. As a direct and proximate cause of Defendants' actions and/or omissions, the Hospitals and Class Members have suffered damages, as alleged herein.

78. But for Defendants' failure to maintain and protect the Hospitals' and Class claims processing and revenue cycle services materials in violation of the parties' understanding of confidence, their materials would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third-parties.

79. The injury and harm the Hospitals and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendants' unauthorized misuse of the Hospitals' and Class Members' materials. Defendants knew their data systems and protocols for accepting and securing the Hospitals' and Class Members' materials had security and other vulnerabilities that placed the Hospitals' and Class Members' materials in jeopardy.

COUNT III

Breach of Implied Contract

80. The Hospitals realleges the allegations above as if fully set forth herein.

81. Through their course of conduct, Defendants, the Hospitals and Class Members entered into implied contracts for Defendants to implement data security and data processing functions adequate to safeguard and protect the Hospitals' and Class Members' claims processing and revenue cycle services materials.

82. Defendants required the Hospitals and Class Members to provide and entrust their claims processing and revenue cycle services materials as a condition of obtaining Defendants' services.

83. Defendants solicited and invited the Hospitals and Class Members to provide their claims processing and revenue cycle service materials as part of Defendants' regular business practices. The Hospitals and Class Members accepted Defendants' offers and provided their claim processing materials to Defendant.

84. The Hospitals and Class Members provided and entrusted their claims processing and revenue cycle services materials to Defendant. In so doing, the Hospitals and Class Members entered into implied contracts with Defendants by which Defendants agreed to ensure that the Hospitals processing materials would not be defective or compromised.

85. A meeting of the minds occurred when the Hospitals and Class Members agreed to, and did, provide their claims processing and revenue cycle services materials to Defendant, in exchange for, amongst other things, the protection of their materials.

86. The Hospitals and Class Members fully performed their obligations under the implied contracts with Defendant.

87. Defendants' breaches caused economic and non-economic harm.

COUNT IV

Breach of the Implied Covenant of Good Faith and Fair Dealing

88. The Hospitals realleges the allegations above as if fully set forth herein.

89. Contracts have an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

90. The Hospitals and Class Members have complied with and performed all conditions of their contracts with Defendants.

91. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices and to process claims and services in a timely and safe manner as a result of the Data Breach.

92. Defendants knew or should have known of the vulnerabilities of the systems that were exploited in the Data Breach.

93. Defendants acted in bad faith and/or with malicious motive in denying the Hospitals and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT V

Breach of Fiduciary Duty

94. The Hospitals s realleges the allegations above as if fully set forth herein.

95. In light of the special relationship between Defendants and the Hospitals and Class Members, whereby Defendants became the guardian of the Hospitals' and Class Members' claim processing materials, Defendants became a fiduciary by their undertaking and guardianship of the materials to act primarily for the Hospitals and Class Members.

96. Defendants have a fiduciary duty to act for the benefit of the Hospitals and Class Members upon matters within the scope of their relationship with Class Members—in particular, to keep their claims processing and revenue cycle service materials secure.

97. Defendants breached their fiduciary duties to the Hospitals and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

98. Defendants breached their fiduciary duties to the Hospitals and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing the Hospitals' and Class Members' claims processing and revenue cycle service materials.

99. Defendants breached their fiduciary duties to the Hospitals and Class Members by failing to timely notify and/or warn the Hospitals and Class Members of the Data Breach.

100. As a direct and proximate result of Defendants' breaches of their fiduciary duties, the Hospitals and Class Members have suffered and will continue to suffer injuries.

COUNT VI

Unjust Enrichment

101. The Hospitals realleges the allegations above as if fully set forth herein. This Count is pled in the alternative to the Breach of Contract Count above.

102. Upon information and belief, Defendants fund their data-security measures entirely from their general revenue, including payments made by or on behalf of the Hospitals and Class Members.

103. As such, a portion of the payments made by or on behalf of the Hospitals and Class Members is to be used to provide a reasonable level of data security, and the amount of each payment allocated to data security is known to Defendants.

104. The Hospitals and Class Members conferred a monetary benefit to Defendant. Specifically, they purchased goods and services from Defendants and/or their agents and provided Defendants with their claims processing and revenue cycle service materials. In exchange, the Hospitals and Class Members should have received from Defendants the goods

and services that were the subject of the transaction and have their processing and service materials protected with adequate data security.

105. Defendants knew that the Hospitals and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the claims processing and revenue cycle service materials of the Hospitals and Class Members for business purposes.

106. Defendants enriched themselves by saving the costs it reasonably should have expended in data-security measures to secure the Hospitals' and Class Members' claims processing materials. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profits at the expense of the Hospitals and Class Members.

107. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to the Hospitals and Class Members, because Defendants failed to implement appropriate data management and security measures mandated by industry standards.

108. If the Hospitals and Class Members knew that Defendants had not reasonably secured their claims processing materials, they would have avoided transacting business with Defendants.

109. As a direct and proximate result of Defendants' conduct, the Hospitals and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

110. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of the Hospitals and Class Members, proceeds that it unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that the

Hospitals and Class Members overpaid for Defendants' services.

PRAYER FOR RELIEF

WHEREFORE, the Hospitals, and each member of the proposed Class respectfully requests that the Court enter judgment in their favor and for the following specific relief against Defendants as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed Class and/or any other appropriate Class under Fed. R. Civ. P. 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of the Hospitals' counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendants, ordering it to cease and desist from similar unlawful activities;

4. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein and from refusing to issue prompt, complete, and accurate disclosures to the Hospitals and Class Members;

5. For injunctive relief requested by the Hospitals, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of the Hospitals and Class Members;

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

8. For all other Orders, findings and determinations identified and sought in this Complaint.

JURY DEMAND

The Hospitals, individually and on behalf of the Class, hereby demands a trial by jury for all issues triable by jury.

Dated: May 16, 2024.

Respectfully submitted,

/s/ *Charles Barrett*
Aubrey Harwell
Trey Harwell
Charles Barrett
Simon N. Levitsky
Daniella Bhadare-Valente
NEAL & HARWELL, PLC
1201 Demonbreun St.
Suite 1000
Nashville, TN 37203
(615) 244-1713
aharwell@nealharwell.com
trey@nealharwell.com
cbarrett@nealharwell.com
slevitsky@nealharwell.com
dbhadare-valente@nealharwell.com

Charles J. LaDuca
Brendan S. Thompson
Christian Hudson
CUNEO GILBERT & LADUCA, LLP
4725 Wisconsin Avenue NW, Suite 200
Washington, DC 20016
(202) 789-3960
charlesl@cuneolaw.com
brendant@cuneolaw.com
chudson@cuneolaw.com

Don Barrett
David McMullan
BARRETT LAW GROUP, P.A.
404 Court Square North
P.O. Box 927
Lexington, MS 39095
(662) 834-2488

dbarrett@barrettlawgroup.com
donbarrettpa@gmail.com
dmcmullan@barrettlawgroup.com

Richard R. Barrett
LAW OFFICES OF RICHARD R. BARRETT, PLLC
2086 Old Taylor Rd., Suite 1011
Oxford, MS 38655
(662) 380-5018
rrb@rrblawfirm.net

Attorneys for the Hospitals and the Class